

Received July 3, 2016, accepted July 15, 2016, date of publication August 25, 2016, date of current version September 16, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2602286

# Biometric Behavior Authentication Exploiting Propagation Characteristics of Wireless Channel

NAN ZHAO<sup>1</sup>, AIFENG REN<sup>1</sup>, MASOOD UR REHMAN<sup>2</sup>, (Senior Member, IEEE),  
ZHIYA ZHANG<sup>1</sup>, XIAODONG YANG<sup>1</sup>, AND FANGMING HU<sup>1</sup>

<sup>1</sup>School of Electronic Engineering, Xidian University, Xi'an 710071, China

<sup>2</sup>University of Bedfordshire, Luton, LU1 3JU, U.K.

Corresponding author: X. Yang (xdyang@xidian.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61671349, in part by the Fundamental Research Funds for the Central Universities, in part by the China Postdoctoral Science Foundation, and in part by the Postdoctoral Research Projects Funded in Shaanxi Province.

**ABSTRACT** Massive expansion of wireless body area networks (WBANs) in the field of health monitoring applications has given rise to the generation of huge amount of biomedical data. Ensuring privacy and security of this very personal data serves as a major hurdle in the development of these systems. An effective and energy friendly authentication algorithm is, therefore, a necessary requirement for current WBANs. Conventional authentication algorithms are often implemented on higher levels of the Open System Interconnection model and require advanced software or major hardware upgradation. This paper investigates the implementation of a physical layer security algorithm as an alternative. The algorithm is based on the behavior fingerprint developed using the wireless channel characteristics. The usability of the algorithm is established through experimental results, which show that this authentication method is not only effective, but also very suitable for the energy-, resource-, and interface-limited WBAN medical applications.

**INDEX TERMS** Wireless body area networks, physical layer security, wireless channel characteristics, authentication.

## I. INTRODUCTION

Wireless body area networks (WBANs) have seen massive level of growth in the recent past [1], [2]. Applications of the WBANs range from communication to navigation, surveillance to sport monitoring and remote health care to networking. It is envisaged that the market of global wearable devices will see shipment of 187.2 million units annually by 2020 [3]. Massive development of the WBANs is a result of rigorous research on multiple aspects including antenna design [4], [5], use of MIMO techniques [6], numerical modeling of the human body [7], propagation mechanism [8] and radio channel modeling [9]–[11]. The WBANs use a number of technologies including Bluetooth, ZigBee, UWB and terahertz for the wireless communications [12]. The advancements in biomedical systems and signal processing techniques have helped greatly to improve the health sector significantly [13]. Continuous development of the healthcare systems is taking them towards a future where prevention, prediction, personalization and participation would be the integral parts of any medical treatment [14]. Sustainability of

current healthcare systems depends on the efficient performance of a number of wearable and implantable wireless sensors. The nature of the applicability makes miniaturization, low complexity and energy efficiency as their prime requirements [3]. Wireless Body Area Networks (WBANs) are trying to meet these requirements while providing economical real-time patient health monitoring and reporting systems thanks to advancements in microelectronics.

The WBAN sensors collect the Personal Health Information (PHI) of a patient in the form of vital physiological parameters such as pulse rate, heartbeat, blood pressure, vision, electrocardiogram, diabetes, and oxygen level. The PHI serves not only as an important reference in medical diagnosis and treatment of the patient; it can also be used as personal identification and health indicator in industry services like insurance. Any theft and misuse of this information can result in serious identity crisis and have fatal consequences for the patient. Availability of high level of security and privacy measures is therefore, pivotal to the

success of the WBAN systems due to very sensitive nature of information they are dealing with [15]. Security flaws can greatly hinder the popularity of the WBANs and affect their development [16].

The WBANs are currently not considering security vulnerabilities fully as more focus is on reliable deployment of these systems [17]. Simple security methods available are not very efficient and attackers can target the wearable/implantable sensors almost effortlessly to compromise them on physical layer [18], [19]. Provision of a simple and efficient authentication mechanism with minimum energy consumption is therefore necessary for the WBAN healthcare systems. In [20], the authors have proposed a light-weight authentication scheme suitable for hierarchical WBANs. This scheme make use of the cryptographic hash function, and symmetric key encryption/decryption algorithms. A new user access control scheme for the WBANs employing a group-based user access ID, an access privilege mask, and a password is proposed in [21]. Ankarali et al. have presented a physical layer authentication method for implantable medical devices (IMDs), which does not need existing cryptology [22]. Gollakota et al. have presented a physical layer security model for the IMDs by delegating its security to a personal base station. The base station acts as a jammer-cum-receiver allowing it to jam the IMD's messages, preventing others from decoding them while being able to decode them itself [23].

The physical layer security and authentication has attracted attention of a number of researchers. Dautov et al. have introduced compressed sensing for wireless physical layer security encryption [24]. Shi has suggested that the pre-shared key in ubiquitous WBAN sensors can be easily stolen due to high demand and inexperienced users, so the node authentication mechanism should have minimal dependency on encryption [25]. This combined with low power consumption requirement makes the traditional methods inappropriate for the WBAN systems.

This paper presents a new physical layer authentication technique based on the observation of the wireless channel to recognize and form a fingerprint of the patient's behavior. This technique not only meets the essential criteria long battery life, adaptability, and availability for a good security authentication protocol [26] but also adds another degree of security through personalization as the behavior of the users in a specific scenario can vary significantly from each other resulting in different wireless channel characteristics and hence, different behavioural fingerprint. Implementation of the authentication on the physical layer also removes high overhead and processing time required for higher-layer security techniques.

Following the introduction in this section, the rest of the paper is structured into four sections. Section II discusses the basics of the proposed algorithm. Section III describes the experimental setup while Section IV presents the measurement results and discussion on the performance of the algorithm. Conclusions are drawn in Section V.

## II. SCENE DESCRIPTION AND PRELIMINARY KNOWLEDGE

The structure of a generic healthcare system is illustrated in Fig. 1. This simple scenario consists of three major parts; collection of the PHI data via body-worn WBAN sensors, data transfer and storage in the medical data cloud and delivery of this data to relevant hospitals and medical staff like doctors simultaneously for real-time monitoring and examination. This work keeps its focus on the collection of the PHI in an indoor environment like home or office (region marked as 'a' in Fig. 1), which is the most important part of this system as overall performance depends on the efficient, and reliable data collection.

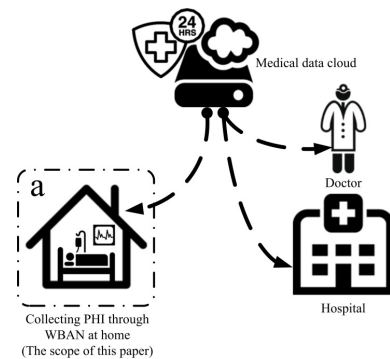


FIGURE 1. Structure of a generic healthcare system.

To implement the proposed authentication algorithm using patient's behavioral fingerprint based on the physical characteristics of the wireless channel, a three level security is established. These three levels are termed as non-trust region, limited trust region, and trust region and are shown in Fig. 2.

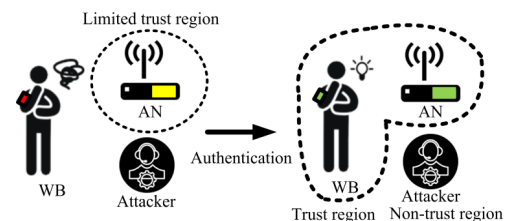


FIGURE 2. The proposed three levels of security in a generic healthcare system.

The non-trust region contains all open nodes in their initial unauthenticated state. In the limited trust region, the nodes undergo some basic security measures, but still vulnerable to the security breaches and attacks. The nodes can enter to the trust region only after extensive authentication process.

The authentication node (AN) serves as a communication base station in the healthcare system and collects the information provided by various wearable bio-sensors (WBs). The AN is a fixed installation and equipped with basic security measures, but still can suffer from security attacks. Therefore, it is placed in limited-trust region. The WBs are being worn by the patient and can be an easy target for the attackers. They are, therefore, considered to be in the non - trust region.

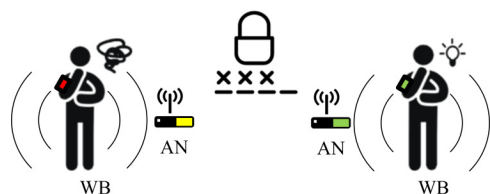


FIGURE 3. Authentication process and entry to trust region of AN and WB.

Fig. 3 depicts the states of WB and AN before and after the authentication process. Initially without any authentication, body-worn WB is in non-trust region (red) while AN is in the limited-trust region (yellow). For the authentication, a template is used based on the observation of the user's behavior. When the user's behavior fingerprint is in accordance with the template of the legal user, AN can enter the trust region, marked as green. When the WB passes the user's two-way authentication, it can also enter the trust region, marked as green also. When both the AN and WB have completed the authentication process, a secure channel is established between them and the two sides can start transmission and reception of the PHI in the trust region.

To further enhance the security of the authentication mechanism and error mitigation, the behavioral fingerprint considers user's habits in four medical scenarios, including body temperature measurement, washing gargle, taking medicine and drip intake as given in Fig. 4.

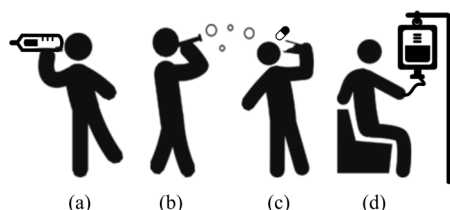


FIGURE 4. Four scenarios considered for the behavioral fingerprint used in the authentication process, (a) body temperature observation, (b) washing gargle, (c) taking medicine, (d) drip intake.

The template is formed based on the characterization of the wireless channel in these scenarios. To obtain authentication, the user needs to behave normally in these scenarios and match the behavioral fingerprint with the template.

Our work is different from available results using upper protocol. Our work is based on the physical layer communications, which is the bottom layer for WBANs. It is known that there are three kinds of identity authentication: the knowledge, the possession and the inherence. The knowledge-based authentication may be forgotten, the authentication on the basis of possession is easily attacked by the compromiser and there are also some disadvantages for traditional biological characteristics (e.g. For iris and fingerprint, although the precision is high, they are changeless and can't be cancelled). Considering these factors, we use wearable nodes to explore the body area channel characteristics. These characteristics

are seen as RF fingerprint; hence, the identity authentication is achieved.

### III. EXPERIMENTAL SETUP AND MEASUREMENTS

The usability of the proposed authentication technique is established through wireless channel measurements in an indoor WBAN environment. Measurements were taken in the Communication Laboratory at Xidian University and in the Xi'an Electronic and Science University hospital. The participant has worn the WB on his right arm while the AN was fixed on the nearby wall. The characteristics of the wireless channel between the WB and AN for a normal behaving user in the form of Received Signal Strength Indicator (RSSI) have been measured in the four scenarios of body temperature observation, washing gargle, taking medicine and drip intake.

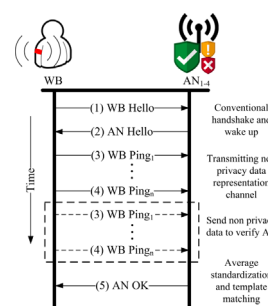


FIGURE 5. Communication protocol used in the proposed algorithm.

The proposed authentication method uses a communication protocol as shown in Fig. 5. At the start of the identity authentication, the sensor worn by the patient initiates the communication with the AN by sending a 'WB Hello' message. This message awakens the AN and it replies with the 'AN Hello' message. On reception of this message, the WB sends the 'WB Ping' message that contains general non-private information such as time alignment, routine detection, etc. The AN calculates the RSSI value from this and subsequent 'WB Ping' messages to form a fingerprint of the wireless channel for the user's action. An RSSI value sequence is then formed out of average of the noted values to standardize the fingerprint. It is then compared to the template for the authentication of the WB and to determine its legitimacy.

In some extreme cases, the security of the AN can also be compromised. This protocol also offers the certification of the AN. The users can make deliberate actions during the 'WB Ping' message with non-private data transmittal that would create significant variations in the wireless channel and hence the fingerprint should not get a match with the template resulting in provision of a failed authentication from the AN. If an authentication is granted instead, it would clearly an indication of a security breach at the AN end. Since, no private health data is yet transmitted by the WB until this point, the communication will be halted and the attacker will get no useful information.

The behavioral template in the form of average standardized value of the raw RSSI will be stored in the AN's





effective calculation. After the preliminary screening of the data, Hamming Distance (HD), which is more accurate than the HWV, is used for the resolution data. It is found in this experiment that the HWV of 2 is a good and practical choice to get the data differentiated, as given below:

$$AN_{BT}[26] \xleftrightarrow{HWV} Template[26] \times \begin{cases} \leq 2, & \text{Calculate HD} \\ > 2, & \text{Authentication Fail} \end{cases} \quad (4)$$

$$AN_{BT}[26] \xleftrightarrow{HD} Template[26] \times \begin{cases} \leq 2, & \text{Authentication Pass} \\ > 2, & \text{Authentication Fail} \end{cases} \quad (5)$$

These equations require that the subject performs the four considered actions in a usual habitual manner so that the collected behavioral data HWV and HD have a value less than 2 in order to get through the authentication.

To analyze the performance of the proposed authentication algorithm, two types of attacks, namely passive attack and active attack are considered. Adversary can eavesdrop on biometric information, active attackers can even break through physical boundaries to simulate the behavior of legitimate users [27]. Figs. 8 and 9, depict the two scenarios of passive attack where the eavesdropper Eve passively eavesdropping Bob and Alice.

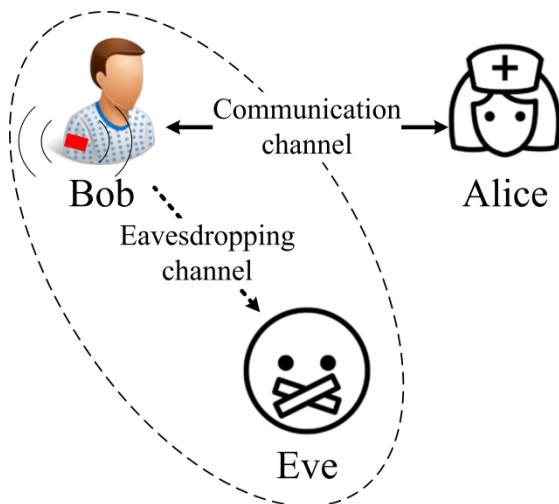


FIGURE 8. Passive eavesdropping on Bob.

The characteristics of both sides of the wireless communication channel are unique [28], [29]. A distance greater than half wavelength can be considered as random, which can be used as a source of random information. In this 2.45GHz system, the distance is very small and it would be impossible for the attacker to obtain the channel information unless he is operating at an arm's length distance that is the rarest possibility. As a result, the eavesdropper Eve would be unable to obtain the RSSI values and the resulting standardized sequenced data. This makes the proposed authentication technique very safe against the passive attacks.

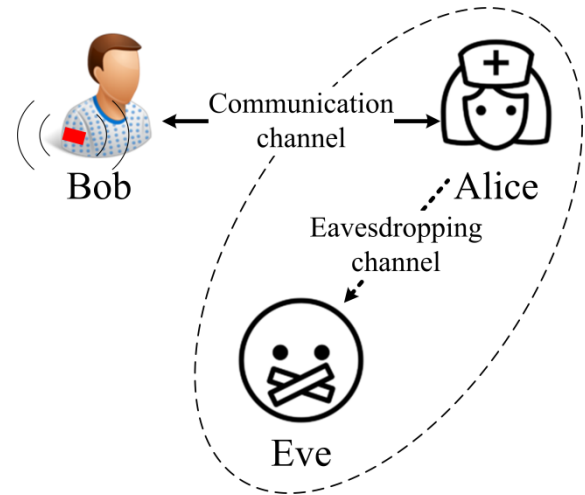


FIGURE 9. Passive eavesdropping on Alice.

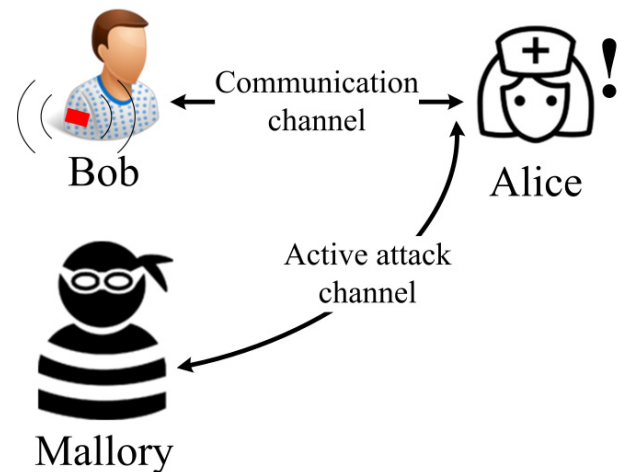


FIGURE 10. Active attack on Alice.

Figs. 10-12 illustrate three possible scenarios of active attacks on the WBAN system.

In Fig. 10, active attacker Mallory, who is pretending to be Bob, initiates an attack on Alice, to get a fake certification. Mallory however, is unable to know the right behavioral fingerprint of Alice and hence, will not be certified.

In Fig. 11, Mallory is now acting as Alice and wishes to gain access to Bob's personal data by deception. However, Bob will get more than one 'AN Hello' responses in this scenario and Mallory's attempt will be uncovered.

A third possibility of the active attack given in Fig. 12 where Mallory uses technical means such as directional antennas to block Alice. In this scenario, Mallory, who is the actual attacker, communicates with Bob (who is legitimate user) in the disguise of Alice. By the AN authentication in the proposed protocol, the attack from Mallory can be found. In addition, since Bob is not static and the authentication time is very short, it is very difficult to carry out shield attack. The efficiency of the proposed technique is evident in these active attack scenarios.

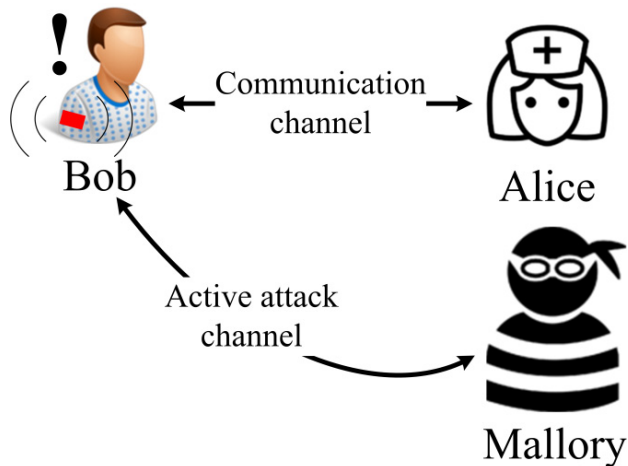


FIGURE 11. Active attack on Bob.

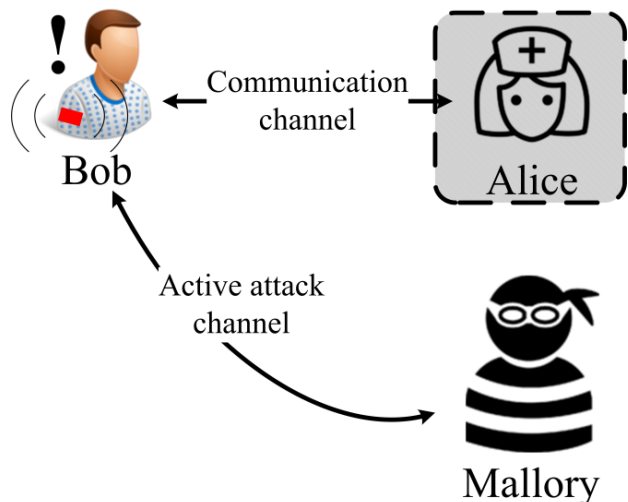


FIGURE 12. Active attack on Bob when Alice is blocked.

Multiple such attack tests were carried out in order to establish the success rate of the proposed authentication protocol. Table 2 provides a summary of the attack tests in the considered passive and active attack scenarios and performance of the proposed authentication method.

The test was carried out to verify the usability of the protocol. The results are good due to the fact that the subjects have more experience than the user do. As preliminary screening, HWV did not show good anti-attack performance, since we are only testing the usability of the protocol. In Table 2, for the four scenarios, all the legitimate users satisfy condition (4) and HD condition (5). After a lot of tests, it is found that the false rejection rate is very low for experienced subjects. False acceptance rate is also very low, both for the experienced and inexperienced subjects. This indicates the commendable and concise usability of the screening process [26], [30].

We also test the passive attack from Eva. Fig. 8-9 presents two modes of attack. Since the distance between spatial distribution of RSSI sequence and Eva is larger than half

TABLE 2. Attack test results for proposed authentication protocol in different passive and active attack scenarios.

Scenario	Alice - Bob		Eve Passive Attack	Mallory Active Attack		
	HWV	HD		(a)	(b)	(c)
Body temperature	14/12	2	Meaningless	Fail	Clash	Fail
Wash gargle	14/12	2	Meaningless	Fail	Clash	Fail
Take the medicine	21/21	0	Meaningless	Fail	Clash	Fail
Drip	22/24	2	Meaningless	Fail	Clash	Fail
Authentication	Pass		Fail	Fail	Fail	Fail

wavelength, they are statistically independent. Eva will only get meaningless random sequence (Table 2) and will not have more knowledge for successful attack.

In the authentication process, the attack from Mallory is extremely dangerous. In this work, we only consider the authentication, the active attack in the communications is out of the scope of the paper.

Fig. 10-12 gives the active attack mode, the anti-attack performance of the protocol is also tested for these three environment. In Table 2(a), since the attacker does not know the behavior fingerprint of the legitimate user, all the attack will fail. In scenario (b), Mallory pretends to be Alice; however, Bob will receive conflict package, the attack would be found. In scenario (c), as there is authentication for Alice, the attack will fail as well. It shows the feasibility of this method to deal with the attack pattern proposed in [23].

All the legitimate users pass the initial screening of HWV and HD. However, subsequent authentication mechanisms bring-in stronger checks and attackers do not get the certification in case of passive and active attack scenarios, in line with the discussion presented earlier in this section. It further affirms the usefulness of the proposed technique.

These results also confirm that this method generates almost no additional packages during the authentication process as compared to upper-layer authentication protocols such as key-based methods. It also brings huge amount of energy saving as no dedicated authentication packets are required. It makes this method very suitable candidate for medical sensor application environment where battery life is a key element of concern.

## V. CONCLUSION

A novel authentication method is implemented on the physical layer based on the observation of user's behavioral fingerprint using wireless channel characterization has been presented. The efficiency of the proposed technique has been analyzed through experimental measurements in realistic WBAN scenarios. Different passive and active attack scenarios have been discussed.

The presented results have shown that the proposed technique provides a higher degree of safety to the WBAN users and safeguard them from most of the security breaches and

increases level of reliability and availability. This method does not require hardware upgrades as long as a wireless communication channel is established between the body-mounted sensors and access nodes making it highly adaptable. Moreover, the proposed algorithm employs normal communication to achieve identity authentication with minimal additional package transmission. It makes it highly energy efficient, resulting in a prolonged battery life of the WBAN sensors. These advantages make this protocol a very well suited authentication method for the WBAN applications.

Further research would be carried out to extend the investigation and optimize the performance of the algorithm by considering different antennas and measuring actual power consumption levels.

## ACKNOWLEDGMENTS

The authors would like to thank the reviewers and the Associate Editor for providing constructive and generous feedback.

## REFERENCES

- [1] D. B. Smith and D. Miniutti, "Cooperative selection combining in body area networks: Switching rates in gamma fading," *IEEE Wireless Commun. Lett.*, vol. 1, no. 4, pp. 284–287, Aug. 2012.
- [2] N. Chahat, C. Leduc, M. Zhadobov, and R. Sauleau, "Antennas and interaction with the body for body-centric wireless communications at millimeter-waves," in *Proc. 7th EUCAP*, 2013, pp. 772–775.
- [3] Q. H. Abbasi, M. Ur Rehman, K. Qaraqe, and A. Alomainy, "Advances in body-centric wireless communication: Applications and state-of-the-art," *IET*, Jul. 2016.
- [4] H. T. Chattha, M. Nasir, Q. H. Abbasi, Y. Huang, and S. S. AlJa'afreh, "Compact low-profile dual-port single wideband planar inverted-F MIMO antenna," *IEEE Antenna Wireless Propag. Lett.*, vol. 12, pp. 1673–1675, Jan. 2014.
- [5] M. Ur-Rehman, Q. H. Abbasi, M. Akram, and C. Parini, "Design of band-notched ultra wideband antenna for indoor and wearable wireless communications," *IET Microw., Antennas Propag.*, vol. 9, no. 3, pp. 243–251, 2015.
- [6] M. Qaraqe, Q. H. Abbasi, A. Alomainy, and E. Serpedin, "Experimental evaluation of MIMO capacity for ultrawideband body-centric wireless propagation channels," *IEEE Antenna Wireless Propag. Lett.*, vol. 13, pp. 495–498, Mar. 2014.
- [7] M. Ur-Rehman, Q. H. Abbasi, X. Chen, and Z. Ying, "Numerical modelling of human body for Bluetooth body-worn applications," *Prog. Electromagn. Res.*, vol. 143, pp. 623–639, Dec. 2013.
- [8] M. Ur Rehman et al., "Investigation of on-body Bluetooth transmission," *IET Microw., Antennas Propag.*, vol. 4, no. 7, pp. 871–880, Jul. 2010.
- [9] Q. H. Abbasi, A. Sani, A. Alomainy, and Y. Hao, "Experimental characterization and statistical analysis of the pseudo-dynamic ultrawideband on-body radio channel," *IEEE Antenna Wireless Propag. Lett.*, vol. 10, pp. 748–751, Aug. 2011.
- [10] Q. H. Abbasi, A. Sani, A. Alomainy, and Y. Hao, "Numerical characterization and modeling of subject-specific ultrawideband body-centric radio channels and systems for healthcare applications," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 2, pp. 221–227, Mar. 2012.
- [11] M. M. Khan, Q. H. Abbasi, A. Alomainy, Y. Hao, and C. Parini, "Experimental characterisation of ultra-wideband off-body radio channels considering antenna effects," *IET Microw., Antennas Propag.*, vol. 7, no. 5, pp. 370–380, Apr. 2013.
- [12] H. Q. Abbasi, H. El Sallabi, N. Chopra, K. Yang, K. A. Qaraqe, and A. Alomainy, "Terahertz channel characterization inside the human skin for nano-scale body-centric networks," *IEEE Trans. THz Sci. Technol.*, vol. 6, no. 3, pp. 427–434, May 2016.
- [13] S. Venugopalan, M. Savvides, M. O. Griofa, and K. Cohen, "Analysis of low-dimensional radio-frequency impedance-based cardio-synchronous waveforms for biometric authentication," *IEEE Trans. Biomed. Eng.*, vol. 61, no. 8, pp. 2324–2335, Aug. 2014.
- [14] J. Andreu-Perez, D. R. Leff, H. M. D. Ip, and G. Z. Yang, "From wearable sensors to smart implants—Toward pervasive and personalized healthcare," *IEEE Trans. Biomed. Eng.*, vol. 62, no. 12, pp. 2750–2762, Dec. 2015.
- [15] D. He, S. Chan, Y. Zhang, and H. Yang, "Lightweight and confidential data discovery and dissemination for wireless body area networks," *IEEE J. Biomed. Health Inform.*, vol. 18, no. 2, pp. 440–448, Mar. 2014.
- [16] V. Mainanwal, M. Gupta, and S. K. Upadhyay, "A survey on wireless body area network: Security technology and its design methodology issue," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIECS)* Coimbatore, India, 2015, pp. 1–5.
- [17] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1635–1657, 3rd Quart., 2014.
- [18] K. Malasri and L. Wang, "Securing wireless implantable devices for healthcare: Ideas and challenges," *IEEE Commun. Mag.*, vol. 47, no. 7, pp. 74–80, Jul. 2009.
- [19] D. He, C. Chen, S. Chan, J. Bu, and P. Zhang, "Secure and lightweight network admission and transmission protocol for body sensor networks," *IEEE J. Biomed. Health Inform.*, vol. 17, no. 3, pp. 664–674, May 2013.
- [20] A. K. Das, S. Chatterjee, and J. K. Sing, "A new biometric-based remote user authentication scheme in hierarchical wireless body area sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 28, nos. 3–4, pp. 221–256, 2015.
- [21] S. Chatterjee, A. K. Das, and J. K. Sing, "A novel and efficient user access control scheme for wireless body area sensor networks," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 26, no. 2, pp. 181–201, 2014.
- [22] Z. E. Ankarali et al., "Physical layer security for wireless implantable medical devices," in *Proc. IEEE Int. Workshop Comput. Aided Modelling Design Commun. Links Netw. (CAMAD)*, Guildford, U.K., Sep. 2015, pp. 144–147.
- [23] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, Aug. 2011.
- [24] R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," *IEEE J. Biomed. Health Inform.*, vol. 20, no. 1, pp. 135–142, Jan. 2016.
- [25] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1803–1816, Sep. 2013.
- [26] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in *Proc. EAI 4th Int. Conf. Wireless Mobile Communication Healthcare (Mobihealth)*, Athens, Greece, 2014, pp. 246–249.
- [27] K. Simoons, J. Bringer, H. Chabanne, and S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 833–841, Apr. 2012.
- [28] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.
- [29] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec. 2014.
- [30] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

**NAN ZHAO**, photograph and biography not available at the time of publication.

**AIFENG REN**, photograph and biography not available at the time of publication.

**MASOOD UR REHMAN** (SM'16) received the B.Sc. degree in electronics and telecommunication engineering from the University of Engineering and Technology, Lahore, Pakistan, in 2004, and the M.Sc. and Ph.D. degrees in electronic engineering from the Queen Mary University of London, London, U.K., in 2006 and 2010, respectively. He joined the Centre for Wireless Research, University of Bedfordshire, University Square, Luton, U.K., as a Lecturer. He was with the Queen Mary University of London as a Post-Doctoral Research Assistant till 2012. His research interests include compact antenna design, radiowave propagation and channel characterization, satellite navigation system antennas in cluttered environment, antenna interaction with human body, body-centric wireless networks and sensors, remote health care technology, mmWave and nano communications for body-centric networks, and body-to-body communications. He has involved in a number of projects supported by industrial partners and research councils. He has contributed to a patent and authored or co-authored two books, five book chapters and over 50 technical articles in leading journals and peer-reviewed conferences. Dr. Rehman is a fellow of the Higher Education Academy, U.K., a member of the IET and part of the technical program committees and organizing committees of several international conferences, workshops, and special sessions. He also serves as a Reviewer for book publishers, the IEEE conferences, and leading journals.

**ZHIYA ZHANG**, photograph and biography not available at the time of publication.

**XIAODONG YANG**, photograph and biography not available at the time of publication.

**FANGMING HU**, photograph and biography not available at the time of publication.

...